Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

Proalpha

Präambel

Diese Vereinbarung zur Auftragsverarbeitung spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung der personenbezogenen Daten des Kunden (nachfolgend „Auftraggeber" genannt) durch eine Gesellschaft der Proalpha Gruppe (nachfolgend „Auftragnehmer" genannt) unter den zwischen den Parteien bestehenden Vertragsverhältnisses regeln. Die Vereinbarung zur Auftragsverarbeitung wird durch Bezugnahme in jeweiligen Vertragsdokumenten zwischen den Parteien rechtswirksam als Anlage in die zwischen den Parteien bestehenden Vertragsverhältnis aufgenommen.

Für Bestandskunden gilt, dass durch das Bereitstellen dieser Vereinbarung vom Auftragnehmer an den Auftraggeber das zwischen den Parteien bestehende Vertragsverhältnis rechtswirksam ergänzt und somit zwischen den Parteien rechtsverbindlich vereinbart wird.

Der Auftraggeber hat den Auftragnehmer mit der Bereitstellung von Services aus dem Produkt- und Serviceportfolio der Proalpha-Gruppe beauftragt. In diesem Zuge verarbeitet der Auftragnehmer auch personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1) Beratung, Implementierung, Betreuung, Support, Wartung und Präsentationen der ERP Software Proalpha mit allen Modulen sowie das erweiterte Softwareangebot, das durch Proalpha vertrieben und implementiert wird. Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich im Weiteren aus **Anlage 1**.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Hauptvertrag und den Folgeaufträgen und auf die hier verwiesen wird (im Folgenden „Hauptvertrag").

2 Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

Die Art der personenbezogenen Daten ergibt sich aus **Anlage 1**.

(2) Kreis der betroffenen Personen:

Der Kreis der betroffenen Personen ergibt sich aus **Anlage 1**.

3 Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage 3** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber über das Trustcenter mitzuteilen.

7 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung zur Hinzuziehung von Subunternehmern: Die Liste **(Anlage 2)** findet sich im Trustcenter unter ***https://www.Proalpha.com/de/trustcenter***. Über den geplanten Einsatz eines weiteren Subunternehmers oder den Austausch eines bestehenden Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab über das Trustcenter zu informieren. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers.

Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und die vom Verantwortlichen genehmigten Subdienstleister findet grundsätzlich in Mitgliedstaaten der Europäischen Union, Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und/oder solchen Ländern statt, für die ein gültiger, auf die Verarbeitung anwendbarer Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 3 DSGVO vorliegt. Es ist dem Auftragsverarbeiter gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb der EU/ des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und sicherstellt, dass beim jeweiligen Subunternehmer ein angemessenes

Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Die Regelung aus 7 (2) dieser Vereinbarung gilt somit auch für die Beauftragung von Subdienstleistern im Drittstaat.

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9 Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten auf Anfrage zum Zweck der direkten Kontaktaufnahme mit.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO. Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist diejenigen Auskünfte zu erteilen, die zum Nachweis der Einhaltung der Pflichten unter diesem Auftragsverarbeitungsvertrag sowie zum Nachweis der technischen und organisatorischen Maßnahmen erforderlich sind. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen. Der Auftraggeber hat dem Auftragnehmer den durch die Erteilung der Auskünfte entstehenden Aufwand zu vergüten.

12 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz, oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1: Angaben zur Datenverarbeitung
- Anlage 2: Genehmigte Subunternehmer unter ***https://www.Proalpha.com/de/trustcenter***
- Anlage 3: Technische und organisatorische Maßnahmen

Anlage 1

Angaben zur Datenverarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Der Auftragnehmer erbringt für den Aufraggeber unterschiedliche Dienstleistungen aus dem Produkt- und Serviceportfolio der Proalpha-Gruppe in der Funktion eines Generalunternehmers. Diese Anlage 1 enthält die auftragsspezifischen Leistungen und Datenverarbeitung i.S.d. Art. 28 Abs. 3 S. 1 DSGVO für die jeweils vom Auftragnehmer erbrachten Services.

Die für diese Vereinbarung geltenden Angaben richten sich stets nach den konkreten Services, die Inhalt des zwischen den Parteien geschlossenen Hauptvertrags sowie ergänzender Vereinbarungen sind.

Proalpha ERP

Der Auftragnehmer stellt dem Auftraggeber eine Softwaresuite zur Verfügung, in welcher dieser personenbezogene Daten verarbeitet. Im Zuge der Implementierung der Lösung sowie im Falle von Supportleistungen hat der Auftragnehmer Zugriff auf die Systeme des Auftraggebers. Ein Zugriff auf personenbezogene Daten des Auftraggebers kann hierbei nicht ausgeschlossen werden.

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Fernzugriff im Rahmen der Implementierung, der Entwicklung, des Supports und der Wartung der Systeme	Alle Daten, die im Rahmen der Proalpha-Systeme durch den Auftraggeber verarbeitet werden	Alle Betroffenen, deren Daten im Rahmen der Proalpha-Systeme durch den Auftraggeber verarbeitet werden	Unterstützung bei Implementierung, Fehlerbehebung und Support, Wartung und Update der Systeme

Proalpha Business Cloud / Full Cloud Experience / Proalpha Cloud Platform Services

Der Auftragnehmer stellt dem Auftraggeber Server und Dienste für Proalpha und die Produkte der Proalpha Gruppe zur Verfügung. Auf den Umfang und die Art der durch den Auftraggeber bearbeiteten Daten hat der Auftragnehmer keinen Einfluss.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Bereitstellung und Wartung von Servern und Diensten für Proalpha und die Produkte der Proalpha Gruppe.	Alle Daten, die im Rahmen der Cloud-Systeme durch den Auftraggeber verarbeitet werden	Alle Betroffenen, deren Daten im Rahmen der Cloud-Systeme durch den Auftraggeber verarbeitet werden	Betrieb der Proalpha Cloud-Lösung für den Auftragnehmer

Proalpha Business Intelligence und NEMO

Der Auftragnehmer stellt dem Auftraggeber eine Lösung zur Visualisierung von Prozessen und vorhandenen Datenbanken zur Verfügung. Über die Art der zu visualisierenden Daten entscheidet alleine der Auftraggeber.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Nutzung der Visualisierungslösung „Qlik“	Alle Daten, die Bestandteil eines Visualisierungsauftrags durch den Auftraggeber sind.	Alle Betroffenen, deren Daten Bestandteil eines Visualisierungsauftrags durch den Auftraggeber sind.	Daten- und Prozessvisualisierung
Nutzung der Visualisierungslösung „Analyzer“	Alle Daten, die Bestandteil eines Visualisierungsauftrags durch den Auftraggeber sind.	Alle Betroffenen, deren Daten Bestandteil eines Visualisierungsauftrags durch den Auftraggeber sind.	Daten- und Prozessvisualisierung
NEMO-Module: Aufbau von Datenstrukturen nach Weisung des Auftraggebers; Anonymisierung von Datensätzen zum Zwecke der Analyse nach Weisung des Auftraggebers	Alle Daten, die im Rahmen der auftraggeberseitig bereitgestellten Datenstrukturen verarbeitet werden.	Beschäftigte des Auftraggebers	Konfiguration von Analysefaktoren. Entspricht dem jeweils vom Auftraggeber im Einzelfall festgelegten Zweck.

Proalpha Academy

Der Auftraggeber nutzt das Angebot der Proalpha Academy, um Nutzern systemspezifische Fachschulungen bereitzustellen und deren Durchführung zu dokumentieren.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck

Bereitstellung von E-Learning-Angeboten	Personenstammdaten Lernfortschritt	Nutzer des E-Learning-Angebots	Durchführung und Dokumentation von fachlichen Schulungen

L-Mobile CRM / Sales

Der Auftraggeber stellt dem Auftragnehmer eine Lösung zum Betrieb eines Customer Relationship Management (CRM) zur Verfügung.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Management von Kundendaten nach Wunsch und konkreter Nutzung des Auftraggebers	Kundenstammdaten (z.B. Name, Adresse) Kommunikationsdaten (z.B. Telefonnummer, E-Mail-Adresse, Faxnummer) Kontakt-/Kundennummer Sonstige Informationen, die der Auftraggeber bei Nutzung des Systems verarbeitet	Kunden Ansprechpartner Sonstige Betroffene, deren Daten der Auftraggeber bei Nutzung des Systems verarbeitet	Übertragung von relevanten Benutzerinformationen zwischen der Proalpha ERP-Suite und Endgeräten des Auftraggebers
Wartung und Pflege der L-Mobile-Anwendungen	Personalstammdaten Kommunikationsdaten Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie Log-Daten Geokoordinaten Firmendaten Vertriebsdaten Materialstammdaten Kundenstammdaten Lieferantenstammdaten Bewegungsdaten (Umlagerungen, Bestandskorrekturen, Inventuren) Datenarten in Abhängigkeit der Nutzung des Systems durch die verantwortliche Stelle	Beschäftigte des Auftraggebers Kunden des Auftraggebers Interessenten des Auftraggebers Lieferanten Handelsvertreter Betroffene in Abhängigkeit der Nutzung des Systems durch die verantwortliche Stelle	Einrichtung, Wartung, Fehlerbehebung zu Anwendungen der L-mobile Anwendungen auf Systemen des Auftraggebers bzw. auf Systemen von Kunden des Auftraggebers.

L-Mobile Warehouse

Der Auftraggeber stellt dem Auftragnehmer eine Lösung zum Betrieb einer Warehouse-Schnittstelle im Bereich der Produktion zur Verfügung. Diese dient dem Austausch relevanter Benutzerdaten, Voreinstellungen und erteilter Berechtigungen an Endgeräte des Auftraggebers.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Rechteverwaltung	Userdaten (z.B. Log-In-Informationen) Bevorzugte Sprache Benutzerrechte	Benutzer der Endgeräte	Übertragung von relevanten Benutzerinformationen zwischen der Proalpha ERP-Suite und Endgeräten des Auftraggebers
Wartung und Pflege der L-Mobile-Anwendungen	Personalstammdaten Kommunikationsdaten Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie Log-Daten Geokoordinaten Firmendaten Vertriebsdaten Materialstammdaten Kundenstammdaten Lieferantenstammdaten Bewegungsdaten (Umlagerungen, Bestandskorrekturen, Inventuren) Datenarten in Abhängigkeit der Nutzung des Systems durch die verantwortliche Stelle	Beschäftigte des Auftraggebers Kunden des Auftraggebers Interessenten des Auftraggebers Lieferanten Handelsvertreter Betroffene in Abhängigkeit der Nutzung des Systems durch die verantwortliche Stelle	Einrichtung, Wartung, Fehlerbehebung zu Anwendungen der L-mobile Anwendungen auf Systemen des Auftraggebers bzw. auf Systemen von Kunden des Auftraggebers.

DIG

Der Auftragnehmer betreibt unter der Bezeichnung „clevercure“ verschiedene Applikationen, hinsichtlich deren Nutzung ein Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer besteht. Diese Applikationen betreffen insbesondere den Bereich „Supply Chain Management“, u.U. aber auch andere Bereiche im Unternehmen des Auftraggebers. Einzelne Applikationen umfassen auch Dokumentenmanagement-Funktionalitäten, wobei die Art und der Umfang der Nutzung bzw. Einstellung der Applikationen in der Entscheidung des Auftraggebers und somit in dessen Sphäre liegt.

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Operative Module: Austausch personenbezogener Daten zwischen beschaffendem Unternehmen und Lieferanten	Userdaten (insbes. Name, E-Mail-Adresse)	Beschäftigte des Auftraggebers Beschäftigte des Lieferanten	Benutzerverwaltung und Bereitstellung von Funktionalitäten
Dispoengine, cleverconnect: Bereitstellung von Schittstellen zwischen den Systemen des Auftraggebers und der Lieferanten zum Betrieb der operativen Module	Userdaten (insbes. Name, E-Mail-Adresse)	Beschäftigte des Auftraggebers Beschäftigte des Lieferanten	Automatisierte Kommunikation zwischen den Systemen des Auftraggebers und der Lieferanten
Strategische Module: Aufbau von Datenstrukturen nach Weisung des Auftraggebers; Erstellung von Workflows nach Weisung des Auftraggebers	Sämtliche Daten, die im Rahmen der auftraggeberseitig erstellten Datenstrukturen und Workflows verarbeitet werden.	Sämtliche Personen, deren Daten im Rahmen der auftraggeberseitig erstellten Datenstrukturen und Workflows verarbeitet werden.	Entspricht dem jeweils vom Auftraggeber im Einzelfall festgelegten Zweck.

Tisoware / Atoria – the people software GmbH

Der Auftragnehmer installiert, implementiert und wartet Softwaresysteme aus der Produktpalette der Atoria – the people software GmbH für den Auftraggeber und erbringt Werk- und/oder Dienstleistungen gemäß Vertragsvereinbarung des bestehenden Hauptvertrags. Diese Wartungsarbeiten und Dienstleistungen können vor Ort beim Auftraggeber oder mittels Fernwartung und Kundenbetreuung durch den Auftragnehmer erfolgen.

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Zugriff auf Kundensysteme vor Ort oder per Fernwartung im Rahmen des Einsatzes der Software der tisoware	Personenstammdaten (z.B. Name, Vorname, Personalnummer) Zeiterfassungsdaten (z.B. Kommen-, Gehen-, Pausenzeiten) Personaleinsatzplanungsdaten (z.B. Schichten, Schichtmodelle, Urlaubsanträge, Abwesenheiten) Personendaten in Verbindung mit Betriebs- und Maschinendaten (Auftragsbeginn, Details zur Auftragsdurchführung) Kantinendaten in Verbindung mit Personendaten (Konsumation) Zutrittsdaten (z.B. Name, Vorname, Zutrittszeit/-ort) Besucherdaten (z.B. Name, Vorname, Firma, Besuchszeiten) Reisedaten in Verbindung mit Personendaten Kommunikationsdaten (z.B. Telefon/Mail) Vertragsstammdaten (Vertragsbeziehung, Produkt- und Vertragsinteresse) Kundenhistorie Vertragsabrechnungs- und Zahlungsdaten	Beschäftigte des Auftraggebers	Beratung, Software-Installation und -Wartung sowie Support (inkl. Fernwartung)

Böhme & Weihs

Der Auftragnehmer erbringt Leistungen auf dem Gebiet der Softwarepflege, -Wartung und -Aktualisierung für die jeweils bereitgestellten Systeme „CASQ-it“ und/oder „MESQ-it“. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich in Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung).

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Zugriff auf Kundensysteme vor Ort oder per Fernwartung im Rahmen des Einsatzes der Dienste „CASQ-it“ und „MESQ-it“	Personenstammdaten Kommunikationsdaten (z. B. Telefon, Email) Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie Vertragsabrechnungs- und Zahlungsdaten Planungs- und Steuerungsdaten Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen) Produktdaten im Kundeneinsatz	Kunden des Auftraggebers Interessenten des Auftraggebers Beschäftigte des Auftraggebers Lieferanten des Auftraggebers	Pflege des CAQ-Systems des Auftraggebers, Programmänderungen, Behebung von Softwarefehlern, Bereitstellung von Updates

Corporate Planning

Der Auftragnehmer erbringt auf Wunsch des Auftraggebers Training & Consulting-Leistungen oder Unterstützungsleistungen durch Support & Wartung (inkl. Fernwartung) von Systemen im Zusammenhang mit der Softwarelösung des Auftragnehmers. Hierbei kann ein Zugriff auf und die Kenntnisnahme von personenbezogenen Daten nicht ausgeschlossen werden.

Der Auftragnehmer stellt darüber hinaus auf Wunsch des Auftraggebers eine Cloud-Infrastruktur zum Betrieb der Softwarelösung des Auftragnehmers zur Verfügung.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Training & Consulting	Daten, die der Auftraggeber innerhalb der Systeme verarbeitet, auf die der Auftragnehmer im Rahmen der geschuldeten Leistung Zugriff hat.	Betroffene, deren Daten innerhalb der Systeme verarbeitet werden, auf die der Auftragnehmer im Rahmen der geschuldeten Leistung Zugriff hat.	Durchführung von Trainings- und Consultingmaßnahmen mit eventuellem Zugriff auf personenbezogene Daten des Auftraggebers
Support und Wartung (inkl. Fernwartung)	Daten, die der Auftraggeber innerhalb der Systeme verarbeitet, auf die der Auftragnehmer im Rahmen der geschuldeten Leistung Zugriff hat.	Betroffene, deren Daten innerhalb der Systeme verarbeitet werden, auf die der Auftragnehmer im Rahmen der geschuldeten Leistung Zugriff hat.	Durchführung von Support und Wartung beim Einsatz der überlassenen Software gemäß Leistungsvereinbarung mit eventuellem Zugriff auf personenbezogene Daten des Auftraggebers
Corporate Planning Cloud	Daten, die der Auftraggeber innerhalb der CP Cloud verarbeitet.	Betroffene, deren Daten der Auftraggeber innerhalb der CP Cloud verarbeitet	Bereitstellung einer Cloud-Infrastruktur

(Insiders) smart INVOICE

Der Auftragnehmer stellt eine Lösung zur Digitalisierung von Eingangsrechnungen zur Verfügung. Hierbei werden wesentliche Inhalte von Eingangsrechnungen erfasst und durch einen Algorithmus alle relevanten Rechnungsdaten extrahiert. Die so erfassten Daten können dann mit weiteren Geschäftsprozessen verknüpft werden. Regelmäßig werden hierbei keine personenbezogenen Daten verarbeitet. Bei Nutzung dieser Funktion kann es allerdings in Einzelfällen nicht ausgeschlossen werden, dass personenbezogene Daten von natürlichen Personen in der Funktion von Rechnungsstellern oder -empfängern durch das System verarbeitet und erfasst werden.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Analyse von Rechnungspositionen in Eingangsrechnungen	Personenstammdaten	Rechnungssteller / -empfänger, soweit es sich um natürliche Personen handelt.	Erkennung und Extraktion relevanter Rechnungsfelder für den Import in verbundene Systeme.

SAGE

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Produktsupports für Services aus dem Produktportfolio der Sage GmbH. Bei der Erbringung von Supportdienstleistungen besteht unter Umständen ein Zugriff auf Systeme des Auftraggebers. Dabei kann eine Kenntnisnahme von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer nicht ausgeschlossen werden.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Durchführung von Supportdienstleistungen inkl. Fernzugriff und Produktupdates	Alle Daten, die im Rahmen der SAGE-Systeme durch den Auftraggeber verarbeitet werden	Alle Betroffenen, deren Daten im Rahmen der SAGE-Systeme durch den Auftraggeber verarbeitet werden	Unterstützung bei Fehlerbehebung, Produktupdates und sonstigen Supportleistungen

Empolis

Der Auftragnehmer stellt unter der Bezeichnung „Proalpha connected knowledge“ eine Cloud-Lösung zum Aufbau einer zentralen Wissensbasis bereit. Der Einsatz dieses KI-basierten Wissensmanagementsystems ermöglicht es, Daten und Dokumente aus verschiedenen Systemen des Auftraggebers in einer einheitlichen Umgebung einfach durchsuchbar zu machen. Die angebundenen Datenquellen, bspw. Proalpha DMS, lokale Fileshares, Sharepoint-Bereiche, Daten aus abgelösten Altsystemen bestimmt der Auftraggeber. Zusätzlich unterstützt die Cloud-Lösung die einfache Erstellung und den Austausch von Expertenwissen.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Anlage und Verwaltung von Nutzerkonten und Erstellung von Experten-Communities.	Konto- und Zugriffsdaten	Benutzer des Systems, die durch Beauftragte des Auftraggebers definiert werden.	Benutzerverwaltung und Bereitstellung von Funktionalitäten des Wissensmanagementsystems durch Beauftragte des Auftraggebers.
Indexierung und semantische Verknüpfung von Dokumenten und Wissensartikeln	Dokumente und Datensätze aus angebundenen Systemen des Auftraggebers	Beschäftigte des Auftraggebers Kunden des Auftraggebers Interessenten des Auftraggebers Lieferanten des Auftraggebers	Einfacher Zugriff auf dokumentiertes Wissen innerhalb des Unternehmens

Anlage 2

Subunternehmerliste, siehe https://www.Proalpha.com/de/trustcenter

Anlage 3

Technische und organisatorische Maßnahmen

Die Proalpha-Gruppe verfolgt ein übergreifendes Standortsicherheitskonzept. Dieses ist, mit Ausnahme einer standortspezifischen Zutrittskontrolle, hinsichtlich der weiteren TOM übergreifend verbindlich definiert.

In der hier vorliegenden Beschreibung über den aktuellen Stand der grundlegenden Maßnahmen zum Schutz der Daten wird einschränkend darauf hingewiesen, dass verständlicherweise nicht alle Sicherheitsmaßnahmen im Detail offengelegt werden können. Gerade in Bezug auf Datenschutz und Datensicherheit ist der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar, da der Schutz der Sicherheitsmaßnahmen gegen unbefugte Offenlegung mindestens genauso wichtig ist wie die Sicherheitsmaßnahmen selbst.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Alarmanlage
- Sicherheitsschlösser
- Zutrittsberechtigungskonzept
- Manuelles Schließsystem
- Schließsystem mit Codesperre
- Schlüsselregelung / Schlüsselbuch
- Automatisches Zugangskontrollsystem (Nebeneingänge)
- Chipkarten-/Transponder-Schließsystem
- Rechenzentren mit Standort in Deutschland oder der EU
- Rechenzentren zertifiziert nach ISO 27001
- separate Serverräume
- Hochsicherheitszugang
- Alarmanlage mit Key und Pin
- Viertürenschleusensystem
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Sicherheitspersonal
- Personenkontrolle beim Pförtner / Empfang

- Protokollierung der Besucher / Besucherbuch
- Tragepflicht von Mitarbeiter- / Gästeausweisen

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Getrenntes Gäste-WLAN
- Detaillierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort
- Passwortregelungen
  - Verwendung von individuellen Passwörtern
  - Passwörter mit einer Mindestlänge
  - Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
  - Passworthistorie
- Schlüsselregelung
- Verschlüsselung von mobilen Datenträgern
- Autonome Fernwartung
- Bestandteil des Sicherheitskonzeptes der pA Gruppe
- Zugriff nur per VPN auf internem Server
- Zentrale Änderung der Zugangsberechtigungen durch IT-Verantwortliche
- Protokollierung der Serverzugriffe auf Benutzerebene

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Detailliertes Berechtigungskonzepts
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Festlegung von Datenbankrechten
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten
- anderer Kunden Rechnung trägt
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln.

- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, HHPS)
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Shredder für die sichere Vernichtung von Daten
- Datenschutzboxen für die Entsorgung von vertraulichen Papierdokumenten

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Folgende Aktivitäten werden protokolliert: Hoch- und Herunterfahren von zentralen Rechnern (v.a. Servern und Firewalls)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle und Belastbarkeit

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Testen von Datenwiederherstellung
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Backup- & Recoverykonzept
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, separaten Ort
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen / IT-Räumen

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Kontrollverfahren

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden

5 Technische und Organisatorische Maßnahmen im Home Office

Die Proalpha-Gruppe ermöglicht ihren Mitarbeitern, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, um dem Sicherheitsstandard des allgemeinen Sicherheitskonzeptes zu entsprechen. Dieses gilt, soweit anwendbar und wird um die folgenden Maßnahmen ergänzt.

Die Maßnahmen unterteilen sich in **technische Maßnahmen**, die den Zugang zum System betreffen sowie in **organisatorische Maßnahmen**, die den Umgang des jeweiligen Mitarbeiters mit Daten an seinem Heimarbeitsplatz betreffen.

Technische Maßnahmen

Die nachfolgenden Maßnahmen stellen die zusätzlich ergriffenen Maßnahmen dar. Für den Zugriff auf das System hat Proalpha folgende Maßnahmen getroffen:

- Zugang ausschließlich über dienstliche Endgeräte
- Endgeräte werden IT-seitig regelmäßigen Updates unterzogen
- Applikationen dürfen ausschließlich nach Konsultation der hierfür vorliegenden Whitelist installiert werden. IT-seitig nicht zugelassene Applikationen dürfen nicht installiert werden
- Ein Zugriff erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung
- Windows Clients
  - Endpoint Security
  - Antivirus Software
  - Systemverschlüsselung
  - Proxy zur Domainfilterung
- iOS Clients
  - verwaltet durch Airwatch MDM/Workspace One
    - Kontrolle über das Gerät mit Möglichkeit zum remote „wipe“ bzw. „lock“
  - komplette Verschlüsselung des Gerätes
  - geschützt durch sechsstelligen Pass Code
  - restriction policy
    - nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
    - keine Diagnosedaten an Apple
    - Benutzer kann keinen 3rd-Party Apps manuell vertrauen

Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- Zutritts- und Kontrollrecht des Arbeitsplatzes durch interne beauftragte Prüfer (z.B. Fachkraft für Arbeitssicherheit oder betrieblicher Datenschutzbeauftragter)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel
- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten
- Verpflichtung auf Vertraulichkeit / zur Geheimhaltung
- Verpflichtung, Wohnortswechsel mitzuteilen